# POLITIQUE SUR L'ACCÈS AUX DOCUMENTS DE LA MRC DES MASKOUTAINS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

## (en lien avec la Loi modernisant des dispositions législatives en matière de protection de renseignements personnels (Loi 25))

11 octobre 2023
(Résolution 23-10-259)

# TABLE DES MATIÈRES

# 1. PRÉAMBULE

Dans le cadre de ses activités et de sa mission, la MRC des Maskoutains (la « MRC ») traite des Renseignements personnels, notamment ceux des visiteurs de son site Web, de citoyens et de ses employés. À ce titre, elle reconnait l'importance de respecter la vie privée et de protéger les Renseignements personnels qu'elle détient.

Afin de s'acquitter de ses obligations en la matière, la MRC s'est dotée de la présente Politique. Celle-ci énonce les principes-cadres applicables à la protection des Renseignements personnels que la MRC détient tout au long du Cycle de vie de ceux-ci et aux droits des Personnes concernées.

La protection des Renseignements personnels détenus par la MRC incombe à tous les employés-cadres, professionnels, techniques et de soutien, ainsi qu'au préfet et à tous les autres élus du conseil des maires et leurs suppléants en fonction à la MRC qui traitent ces renseignements. Ces personnes doivent comprendre et respecter les principes de protection des Renseignements personnels inhérents à l'exercice de leurs fonctions ou qui découlent de leur relation avec la MRC.

# 2. OBJET

La présente Politique :

- Énonce les principes encadrant la gouvernance de la MRC à l'égard des Renseignements personnels tout au long de leur Cycle de vie et de l'exercice des droits des Personnes concernées;
- Prévoit le processus de traitement des plaintes relatives à la protection des Renseignements personnels;
- Définit les rôles et responsabilités en matière de protection des Renseignements personnels à la MRC;
- Décrit les activités de formation et de sensibilisation que la MRC offre à son personnel.

# 3. CADRE NORMATIF

La présente Politique s'inscrit dans un contexte régi notamment par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2-1.). Conformément à cette Loi, la présente Politique est accessible via le site Web de la MRC [Documentation | MRC des Maskoutains (mrcmaskoutains.qc.ca)].

# 4. GOUVERNANCE

## 4.1 DÉFINITION

Pour l'interprétation de la présente Politique, à moins que le contexte ne comporte un sens différent, les mots employés ont la signification suivante :

**« Commission d'accès à l'information (CAI) »** : organisme gouvernemental québécois responsable de mettre en œuvre les politiques d'accès à l'information et de protection des renseignements personnels au Québec.

**« Comité »** : Comité sur l'accès à l'information et la protection des renseignements personnels de la MRC.

**« Consentement »** : accord manifeste, libre et éclairé donné par une personne à des fins spécifiques. Le Consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.

**« Cycle de vie »** : ensemble des étapes visant le traitement d'un Renseignement personnel, soit la collecte, l'utilisation, la communication, la conservation et la destruction de celui-ci.

**« Évaluation des facteurs relatifs à la vie privée (ÉFVP) »** : démarche préventive qui vise à mieux protéger les Renseignements personnels et à respecter la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui entraîneraient des conséquences positives et négatives sur le respect de la vie privée des Personnes concernées.

**« Incident de confidentialité »** : tout accès, utilisation ou communication non autorisés par la Loi d'un Renseignement personnel, de même qu'à la perte d'un Renseignement personnel ou à toute autre atteinte à sa protection.

**« MRC »** : MRC des Maskoutains.

**« Loi »** : *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1).

**« Personne concernée »** : personne physique à qui se rapportent les Renseignements personnels.

**« Préjudice sérieux »** : atteinte aux droits fondamentaux des personnes à la protection des Renseignements personnels qui les concernent et de leur vie privée, et met en danger la sécurité, la santé ou le bien-être de ces personnes, ou encore porte atteinte à l'image de marque de la MRC, avec ou sans médiatisation. Porte sur la sensibilité des Renseignements personnels concernés, l'utilisation malveillante possible de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables.

**« Profilage »** : collecte et utilisation de Renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne.

**« Renseignement anonymisé »** : un renseignement personnel est anonymisé quand il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement la Personne concernée.

**« Renseignement dépersonnalisé »** : renseignement qui ne permet plus d'identifier directement la Personne concernée.

**« Renseignement personnel »** : renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier.

**« Renseignement personnel à caractère public »** : renseignement qui permet d'identifier directement une personne, mais qui est public. Sont considérés à caractère public le nom, le titre, la fonction, la classification et l'échelle de traitement rattachée à cette classification, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone du lieu de travail d'un membre de la MRC, de son conseil des maires et suppléants, et de son personnel de direction. Le traitement d'un membre du personnel de la MRC n'est pas un renseignement à caractère public.

**« Renseignement personnel confidentiel »** : Renseignement personnel qui porte sur une personne physique et permet de l'identifier. Ce renseignement est confidentiel. Sa confidentialité découle du droit à la vie privée permettant à toute personne d'exercer un contrôle sur l'utilisation et la circulation de ses renseignements. Sauf exception, ce renseignement ne peut être communiqué sans le Consentement de la Personne concernée.

**« Renseignement personnel sensible »** : renseignement qui, par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée. Par exemple, le renseignement sensible peut concerner la santé ou l'orientation sexuelle; les caractéristiques morphologiques, comportementales ou biologiques (biométrie), le groupe ethnique, les croyances philosophiques ou religieuses, l'état des finances.

**« Responsable de l'accès aux documents (RAD) »** : désigne la personne qui, au sein de la MRC, exerce cette fonction et qui doit répondre aux demandes d'accès aux documents selon la Loi.

**« Responsable de la protection des Renseignements personnels (RPRP) »** : la personne qui, au sein de la MRC, exerce cette fonction et veille à y assurer le respect et la mise en œuvre de la Loi concernant la protection des Renseignements personnels.

### 4.2 Objet et champ d'application

Cette Politique s'applique aux documents détenus par la MRC dans l'exercice de ses fonctions ainsi que la conservation de ses documents, peu importe leur forme : écrite, graphique, sonore, visuelle, informatisée ou autre.

Elle s'applique à tous les employés, ainsi qu'à tous les organismes œuvrant au nom de la MRC, dans le cadre de l'exercice de leurs fonctions, et ce, sans limite de temps, pendant et après la fin de leur relation avec la MRC.

## 5. GESTION DES INCIDENTS DE CONFIDENTIALITÉ

En complément à la définition du terme (voir 4.1 Définition), un Incident de confidentialité pourrait se produire, par exemple, lorsque :

- Un membre du personnel consulte un Renseignement personnel sans autorisation;
- Un membre du personnel communique des Renseignements personnels au mauvais destinataire;

- La MRC est victime d'une cyberattaque : hameçonnage, rançongiciel, etc.

## 5.1 Mesures à adopter et obligations en cas d'Incident de confidentialité

Les étapes qui suivent peuvent être réalisées simultanément :

### 5.1.1 Évaluer la situation

Lorsque la MRC a des raisons de croire que s'est produit un Incident de confidentialité impliquant un Renseignement personnel qu'elle détient doit notamment :

- Établir les circonstances de l'incident;
- Identifier les Renseignements personnels impliqués;
- Identifier les Personnes concernées;
- Trouver le problème, que ce soit une erreur, une vulnérabilité, etc.

Cette évaluation doit se poursuivre tant que tous les éléments n'ont pas été identifiés.

### 5.1.2 Diminuer les risques

La MRC doit prendre rapidement les mesures raisonnables qui s'imposent afin de diminuer les risques qu'un préjudice, qu'il soit sérieux ou non, ne soit causé et pour éviter que de nouveaux incidents de même nature ne surviennent, par exemple :

- Cesser la pratique non autorisée;
- Récupérer ou exiger la destruction des Renseignements personnels impliqués;
- Corriger les lacunes informatiques.

### 5.1.3 Identifier la nature du préjudice

L'objectif consiste à déterminer s'il faut aviser la CAI et les Personnes concernées ainsi qu'établir les mesures à mettre en place pour diminuer les risques notamment :

- Inscrire une note dans les dossiers visés par un risque de vol d'identité;
- Exiger des vérifications supplémentaires.

### 5.1.4 Inscrire l'incident au registre

Identifier si le risque de préjudice est qualifié ou non de sérieux. Voir *Annexe A – Modèle de registre des Incidents de confidentialité*.

### 5.1.5 S'il y a un risque de Préjudice sérieux

La MRC doit :

- **Aviser la CAI dès que possible**, même si elle n'a pas colligé l'ensemble des informations relatives à l'incident, et remplir la déclaration par la suite. Elle peut ainsi aviser la CAI de l'incident et, plus tard, confirmer le nombre de Personnes concernées.
- **Aviser toute personne dont un Renseignement personnel est concerné par l'incident**, à moins que cet avis ne soit susceptible d'entraver une enquête. Un délai peut s'appliquer entre le moment où la MRC prend connaissance de l'incident et celui où il en avise les Personnes concernées. Ce délai peut être nécessaire afin, par exemple, d'identifier les Renseignements personnels impliqués, les Personnes concernées, la faille de sécurité et pour colmater celle-ci ou pour éviter d'entraver une enquête en cours.

Ces avis sont obligatoires. Voir l'*Annexe B – Formulaire de déclaration d'un Incident de confidentialité.*

## 5.2 Communication des Renseignements personnels sans le Consentement

Sous réserve des exceptions prévues par la Loi, la MRC ne peut communiquer des Renseignements personnels sans le Consentement de la Personne concernée. Le Consentement doit être donné expressément lorsque des Renseignements personnels sensibles sont en cause.

Lorsque des Renseignements personnels sont communiqués à un mandataire ou un fournisseur de services dans le cadre d'un mandat ou d'un contrat de service ou pour l'exécution d'un mandat, la MRC doit conclure une entente avec le fournisseur de services ou le mandataire qui comprend les dispositions contractuelles types de la MRC.

Lorsque les Renseignements personnels sont communiqués à des tiers hors Québec, la MRC procède à une ÉFVP conformément à l'article 8 des présentes. Une communication à des tiers est consignée au registre prévu cet effet.

## 5.3 Registre des Incidents de confidentialité

La MRC doit tenir un registre dans lequel elle collige tous les Incidents de confidentialité impliquant des Renseignements personnels. Elle doit y inscrire même les incidents qui ne présentent pas de risques de Préjudice sérieux. À la demande de la CAI, la MRC doit transmettre une copie de son registre.

La MRC doit tenir un registre des Incidents de confidentialité. Le modèle se trouve à l'*Annexe A – Modèle de registre des Incidents de confidentialité.*

La personne responsable de remplir et de communiquer ce registre à la CAI est le RPRP de la MRC.

Le registre des Incidents de confidentialité doit contenir les éléments suivants :

- Une description des Renseignements personnels visés par l'incident. Si cette information n'est pas connue, la MRC doit inscrire la raison justifiant l'impossibilité de fournir cette description;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu ou une approximation de cette période si elle n'est pas connue;
- La date ou la période au cours de laquelle la MRC a pris connaissance de l'incident;
- Le nombre de Personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;
- Une description des éléments qui amènent la MRC à conclure qu'il y a, ou non, risque qu'un Préjudice sérieux soit causé aux Personnes concernées, comme :
- La sensibilité des Renseignements personnels concernés;
- Les utilisations malveillantes possibles des renseignements;
- Les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables;
- Les dates de transmission des avis à la CAI et aux Personnes concernées, quand l'incident présente le risque de Préjudice sérieux. La MRC doit aussi préciser si elle a donné des avis publics et la raison de ceux-ci;
- Une brève description des mesures prises par la MRC à la suite de l'incident pour diminuer les risques qu'un préjudice soit causé.

Les renseignements du registre doivent être mis à jour et conservés pour une période minimale de cinq ans, après la date ou période de prise de connaissance de l'incident par la MRC.

Dans divers contextes, la MRC peut confier des Renseignements personnels à des tiers qui en assurent la conservation. La MRC demeure malgré tout responsable de l'ensemble de ses obligations en cas d'Incident de confidentialité : mesures à prendre, registre à tenir et à mettre à jour, avis à donner, etc.

# 6. OUTILS D'ÉVALUATION DES PRÉJUDICES ET RISQUES

## 6.1 Critère pour l'évaluation des préjudices, impacts et risques

Lorsque la MRC évalue le risque qu'un préjudice soit causé à une personne dont un Renseignement personnel est concerné par un Incident de confidentialité. La MRC considère notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. Son RPRP doit être consulté.

# 7. INVENTAIRE ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

## 7.1 Inventaire des fichiers de Renseignements personnels

La MRC doit établir et maintenir à jour un inventaire de ses fichiers de Renseignements personnels. Cet inventaire doit contenir :

- La désignation de chaque fichier, les catégories de renseignements qu'il contient, les fins pour lesquelles les renseignements sont conservés et le mode de gestion de chaque fichier;
- La provenance des renseignements versés à chaque fichier;
- Les catégories de Personnes concernées par les renseignements versés à chaque fichier;
- Les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions;
- Les mesures de sécurité prises pour assurer la protection des Renseignements personnels.

Selon le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RLRQ, c. A-2.1, r.2) toute personne qui en fait la demande a droit d'accès à cet inventaire, sauf à l'égard des renseignements dont la confirmation de l'existence peut être refusée en vertu des dispositions de la Loi.

## 7.2 Protection des Renseignements personnels dans les systèmes d'information

### 7.2.1 Identification des étapes du Cycle de vie d'un Renseignement personnel

- Collecte;
- Utilisation;
- Communication;
- Conservation;
- Destruction.

### 7.2.2 Collecte

Première étape du Cycle de vie du Renseignement personnel, la collecte est le moment où le Renseignement personnel est :

- Recueilli (ex. : formulaire d'adhésion, sondage, outils analytiques Web);
- Créé (ex. : nº d'usagers ou d'utilisateurs);
- Inféré (ex. : profil des citoyens ou des municipalités), c'est-à-dire déduit à partir d'autres renseignements.

Le fait de visualiser un Renseignement personnel, comme ceux contenus sur une pièce d'identité, constitue également une collecte, même s'il n'y a pas de conservation par la suite.

La collecte peut être réalisée directement par la MRC ou par un tiers, comme un mandataire ou un partenaire.

À cette étape, les obligations suivantes doivent être respectées afin de protéger les Renseignements personnels :

- Déterminer les fins de la collecte : un intérêt sérieux et légitime doit motiver la constitution d'un dossier sur une personne;
- Limiter la collecte de Renseignements personnels : la collecte doit se limiter aux renseignements nécessaires aux fins déterminées. En cas de doute, un Renseignement personnel est réputé non nécessaire;
- Recueillir les Renseignements personnels par des moyens légaux et légitimes : sauf exception, la collecte doit se faire auprès de la Personne concernée;
- Informer la Personne concernée, avant de constituer un dossier :
    - De l'objet du dossier;
    - De l'utilisation qui sera faite des Renseignements personnels;
    - Des catégories de personnes qui y auront accès au sein de la MRC;
    - De l'endroit où ils seront détenus;
    - De ses droits d'accès et de rectification.
- Obtenir le Consentement des Personnes concernées avant de collecter leurs Renseignements personnels auprès d'un tiers, à moins d'une exception prévue par la Loi.

Sauf exception prévue par la Loi. la MRC ne peut obliger une personne à fournir un Renseignement personnel afin qu'elle obtienne un bien, un service ou un emploi.

### 7.2.3 Utilisation

L'utilisation est la période où le Renseignement personnel est utilisé par les personnes autorisées au sein de la MRC. Un Renseignement personnel ne peut être utilisé au sein de la MRC qu'aux fins pour lesquelles il a été recueilli, à moins du Consentement de la Personne concernée. Ce Consentement doit être manifesté de façon expresse dès qu'il s'agit d'un Renseignement personnel sensible.

À cette étape, la MRC doit respecter les obligations suivantes :

- Limiter l'accès aux Renseignements personnels aux seules personnes ayant la qualité pour les recevoir au sein de la MRC lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions;
- Limiter l'utilisation des Renseignements personnels : à moins d'une exception prévue par la Loi, la MRC doit obtenir le Consentement de la Personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli.

La MRC peut toutefois utiliser un Renseignement personnel à une autre fin sans le Consentement de la personne concernée dans les seuls cas suivants :

- Lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli;
- Lorsque son utilisation est manifestement au bénéfice de la personne concernée;
- Lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi;
- Lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.

Un Renseignement personnel est dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la Personne concernée. La MRC qui utilise des Renseignements dépersonnalisés doit prendre les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de Renseignements dépersonnalisés. La Loi prévoit des sanctions pour toute personne qui procède ou tente de procéder à l'identification d'une personne physique à partir de Renseignements dépersonnalisés sans l'autorisation de la personne les détenant ou à partir de Renseignements anonymisés

### 7.2.4 Communication

La communication est la période où le Renseignement personnel est communiqué, par exemple dans un système de prestation électronique de services, par courriel, au service à la clientèle, par le biais de sites Web, aux ressources humaines ou à un tiers.

À cette étape, la MRC doit respecter les obligations suivantes :

- Obtenir le Consentement des Personnes concernées pour communiquer leurs renseignements à un tiers (ex. : assureur, prestataire de service, organisme gouvernemental, partenaire), à moins d'une exception prévue dans la Loi;
- Respecter les obligations prévues par la Loi lorsqu'elle communique des Renseignements personnels sans le Consentement de la Personne concernée;
- Respecter les obligations particulières applicables à la communication de Renseignements personnels à l'extérieur du Québec.

### 7.2.5 Conservation

La conservation est la période durant laquelle la MRC garde des Renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non.

À cette étape, la MRC doit respecter les obligations suivantes :

- Assurer la qualité des Renseignements personnels en veillant à ce que les Renseignements personnels qu'elle détient soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la Personne concernée;

- Prendre des mesures de sécurité propres à assurer la sécurité des Renseignements personnels.

#### 7.2.6 Destruction

Le Cycle de vie du Renseignement personnel se termine lors de sa destruction.

À cette étape, la MRC doit :

- Détruire les Renseignements personnels de manière sécuritaire dès que la finalité pour laquelle ils ont été collectés est accomplie, sous réserve du délai prévu par la Loi ou par un calendrier de conservation établi par règlement du gouvernement (p. ex. : pour les obligations fiscales).

### 7.3 Autres obligations : sécurité, accès et rectification

Mettre en place des mesures de sécurité propres à assurer la protection des Renseignements personnels collectés, utilisés, communiqués, conservés ou détruits.

- Ces mesures sont raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des Renseignements personnels.

  Permettre l'exercice des droits d'accès et de rectification et répondre avec diligence, dans les 30 jours, aux demandes d'accès aux Renseignements personnels et de rectification soumise par les Personnes concernées.

- L'absence de réponse dans ce délai équivaut à un refus. Un citoyen peut contester un refus ou une réponse jugée insatisfaite en exerçant son droit de recours devant la CAI.

## 8. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (ÉFVP)

La réalisation d'une ÉFVP sert à démontrer que la MRC a respecté toutes les obligations en matière de protection des Renseignements personnels et que toutes les mesures ont été prises afin de protéger efficacement ces renseignements.

### 8.1 Système d'information ou de prestation électronique de services

La MRC doit faire une ÉFVP avant d'entreprendre un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui implique des Renseignements personnels ;

### 8.2 Collecte de Renseignements personnels pour les partenaires

La MRC doit faire une ÉFVP avant de communiquer des Renseignements personnels sans le Consentement des Personnes concernées à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques.

## 8.3 Communication des Renseignements personnels sans le Consentement

La MRC doit faire une ÉFVP avant de communiquer des Renseignements personnels, sans Consentement des Personnes concernées, conformément à l'article 68 de la Loi.

## 8.4 Communication pour des situations définies

La MRC doit faire une ÉFVP avant de recueillir des Renseignements personnels nécessaires à l'exercice des attributions ou à la mise en œuvre d'un programme d'un organisme public avec lequel elle collabore pour la prestation de services ou pour la réalisation d'une mission commune.

## 8.5 Communication à des tiers à l'extérieur du Québec

De plus, lorsque les Renseignements personnels sont communiqués à l'extérieur du Québec, la MRC s'assure que ceux-ci bénéficient d'une protection adéquate, notamment au regard des principes de protection des Renseignements personnels généralement reconnus.

# 9. CONSENTEMENT ET INFORMATION DES PERSONNES

## 9.1 Procédure, portée et durée

La MRC ne recueille que les Renseignements personnels nécessaires à la réalisation de sa mission et de ses activités. Avant de recueillir des Renseignements personnels, la MRC détermine les fins de leur traitement. La MRC ne recueille que les Renseignements personnels strictement nécessaires aux fins indiquées.

Au moment de la collecte, et par la suite sur demande, la MRC informe les Personnes concernées, notamment, des fins et des modalités de traitement de leurs Renseignements personnels et de leurs droits quant à ces renseignements, par exemple, au moyen d'une Politique de confidentialité ou d'un avis « juste-à-temps ».

Lorsque la Loi exige l'obtention d'un Consentement, celui-ci doit être manifeste, libre, éclairé et donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs. Ce Consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

## 9.2 Personne mineure

Les Renseignements personnels concernant une personne mineure de moins de 14 ans ne peuvent être recueillis auprès de celui-ci sans le Consentement du titulaire de l'autorité parentale ou du tuteur, sauf lorsque cette collecte est manifestement au bénéfice de ce mineur.

# 10. COMMUNICATION DES RENSEIGNEMENTS PERSONNELS À DES TIERS SANS CONSENTEMENT

## 10.1 Communication pour l'exécution d'un mandat ou contrat de service

Dans le cadre d'un mandat ou d'un contrat de service, la MRC peut, sans le Consentement de la Personne concernée, communiquer un Renseignement personnel si cette communication est nécessaire

Ne s'applique pas lorsque l'exécutant du contrat est un membre d'un ordre professionnel.

## 10.2 Communication pour des situations définies

La MRC peut, sans le Consentement de la Personne concernée, communiquer un Renseignement personnel :

- À un organisme public ou à un organisme d'un autre gouvernement lorsque cette communication est nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en œuvre d'un programme dont cet organisme a la gestion;
- À un organisme public ou à un organisme d'un autre gouvernement lorsque la communication est manifestement au bénéfice de la personne concernée;
- À une personne ou à un organisme lorsque des circonstances exceptionnelles le justifient;
- À une personne ou à un organisme si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de l'identification de cette personne.

Cette communication s'effectue dans le cadre d'une entente écrite qui indique :<<

- L'identification de la MRC qui communique le renseignement et celle de la personne ou de l'organisme qui le recueille;
- Les fins pour lesquelles le renseignement est communiqué;
- La nature du renseignement communiqué;
- Le mode de communication utilisé;
- Les mesures de sécurité propres à assurer la protection du Renseignement personnel;
- La périodicité de la communication;
- La durée de l'entente.

## 10.3 Communication à des tiers à l'extérieur du Québec

Avant de communiquer à l'extérieur du Québec des Renseignements personnels ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, la MRC s'assurera qu'ils bénéficieront d'une protection équivalant à celle prévue à la présente Loi.

Si la MRC estime que les renseignements visés au premier alinéa ne bénéficieront pas d'une protection équivalant à celle prévue à la présente Loi, elle devra refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte.

# 11. GESTION DU CYCLE DE VIE DES FICHIERS

## 11.1 Processus de destruction ou d'anonymisation

Tout document contenant des informations qui répondent aux définitions de Renseignements personnels, Renseignements personnels confidentiels et Renseignements personnels sensibles, devra être déchiqueté par la firme externe avec qui la MRC fait affaire. Ces documents ne peuvent pas être simplement déchiquetés avec la déchiqueteuse du bureau de la MRC, car ces documents doivent être broyés après avoir été déchiquetés, afin d'éviter tout risque de reconstitution.

Afin de permettre une conservation permanente responsable, certains documents subiront du caviardage, lorsque les Renseignements personnels, Renseignements personnels confidentiels et Renseignements personnels sensibles ne seront pas jugés essentiels à la compréhension ou la pertinence du contenu du document.

Lorsque les fins pour lesquelles un Renseignement personnel a été recueilli ou utilisé sont accomplies, la MRC doit le détruire, ou l'anonymiser pour l'utiliser à des fins d'intérêt public, sous réserve du calendrier de conservation des documents de la MRC en vigueur.

Un renseignement concernant une personne physique est anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne. Les Renseignements anonymisés doivent l'être selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement.

À la lumière des avancées technologiques actuelles et futures, la CAI estime qu'il est quasi impossible de certifier que des Renseignements anonymisés ne pourraient pas éventuellement être réidentifiés. L'anonymisation des Renseignements personnels présuppose des risques d'Incidents de confidentialité. La Loi prévoit aussi des sanctions pour toute personne qui tente d'identifier une personne à partir de Renseignements anonymisés.

# 12. ACTIVITÉS DE RECHERCHE ET ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Des chercheurs peuvent demander l'accès à des Renseignements personnels à des fins de recherche. Une telle demande doit être soumise au RPRP de la MRC.

Lorsque l'ÉFVP conclut que des Renseignements personnels peuvent être communiqués à cette fin, la MRC doit conclure une entente avec les chercheurs qui contient les dispositions contractuelles types de la MRC et toute mesure supplémentaire identifiée dans l'ÉFVP.

## 13. SONDAGE

Toute personne, organisme ou autre organisation qui souhaite effectuer un sondage auprès de Personnes concernées au moyen de Renseignements personnels que détient la MRC doit le faire conformément à une politique de la MRC relative aux sondages.

## 14. DROITS DES PERSONNES CONCERNÉES

### 14.1 Droit

Sous réserve de ce que prévoient les lois applicables, toute Personne concernée dont les Renseignements personnels sont détenus par la MRC dispose notamment des droits suivants :

- Le droit d'accéder aux Renseignements personnels détenus par la MRC et d'en obtenir une copie, que ce soit en format électronique ou non électronique;
  - À moins que cela ne soulève des difficultés pratiques sérieuses, un Renseignement personnel informatisé recueilli auprès d'une Personne concernée, et non pas créé ou inféré à partir d'un Renseignement personnel la concernant, lui est communiqué dans un format technologique structuré et couramment utilisé, à sa demande. Ce renseignement est aussi communiqué, à sa demande, à toute personne ou à tout organisme autorisé par la Loi à recueillir un tel renseignement.
- Le droit de faire rectifier tout Renseignement personnel incomplet ou inexact détenu par la MRC;
- Le droit d'être informée, le cas échéant, que des Renseignements personnels sont utilisés pour prendre une décision fondée sur un traitement automatisé.

### 14.2 Exceptions

Bien que le droit d'accès puisse être exercé en tout temps, l'accès aux documents contenant ces renseignements est assujetti à certaines exceptions identifiées dans la Loi.

### 14.3 Consultation

Les documents contenant des Renseignements personnels peuvent être consultés sur place ou être accessibles d'une autre manière, avec ou sans paiement de frais. Le cas échéant, la MRC informe la Personne concernée de l'obligation de payer des frais avant de traiter sa demande.

### 14.4 Demande d'accès à l'information

Les demandes d'accès aux Renseignements personnels par les Personnes concernées peuvent être faites verbalement ou par écrit. Les demandes verbales seront traitées de manière informelle et peuvent ne pas recevoir de réponse écrite.

Les demandes d'accès aux Renseignements personnels sensibles doivent être faites par écrit et recevront une réponse écrite.

Les demandes d'accès aux Renseignements personnels doivent être suffisamment précises pour permettre au RPRP de localiser lesdits Renseignements personnels. Le droit d'accès ne s'applique qu'aux Renseignements personnels existants.

## 15. TRAITEMENT DES PLAINTES

Toute plainte relative aux pratiques de protection des Renseignements personnels de la MRC ou de sa conformité aux exigences de la Loi qui concernent les Renseignements personnels doit être transmise au RPRP, lequel doit y répondre dans un délai de 20 jours.

## 16. SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS

La MRC met en place des mesures de sécurité raisonnables afin d'assurer la confidentialité, l'intégrité et la disponibilité des Renseignements personnels recueillis, utilisés, communiqués, conservés ou détruits. Ces mesures tiennent notamment en compte du degré de sensibilité des Renseignements personnels, de la finalité de leur collecte, de leur quantité, de leur localisation et de leur support.

La MRC gère les droits d'accès des membres de son personnel afin que seuls ceux soumis à un engagement de confidentialité et ayant besoin d'y accéder dans le cadre de leurs fonctions aient accès aux Renseignements personnels.

## 17. RÔLES ET RESPONSABILITÉS

La protection des Renseignements personnels que la MRC détient repose sur l'engagement de tous les employés-cadres, professionnels, techniques et de soutien, ainsi que le préfet et tous les autres élus du conseil des maires et leurs suppléants en fonction à la MRC, qui traitent ces renseignements, et plus particulièrement des suivants :

### 17.1 Le RPRP

- S'assure de la protection des Renseignements personnels tout au long de leur Cycle de vie, de la collecte à la destruction;
- Siège au Comité;
- Se conforme aux exigences liées aux demandes d'accès ou de rectification, sous réserve des responsabilités dévolues au RAD, y compris :
  - Donner au requérant un avis de la date de réception de sa demande;
  - Aviser le requérant des délais et de son droit à la révision;

- Répondre à la demande dans un délai de 20 jours, ou si le traitement de la demande ne paraît pas possible sans nuire au déroulement normal des activités de la MRC, dans un délai de 10 jours supplémentaires, après avoir avisé le requérant par écrit;
- Prêter assistance au requérant pour identifier le document susceptible de contenir les renseignements recherchés lorsque sa demande est imprécise;
- Motiver tout refus d'acquiescer à une demande d'accès;
- À la demande du requérant, lui prêter assistance pour l'aider à comprendre la décision le concernant;
- Rendre sa décision par écrit et en transmettre une copie au requérant. Elle doit être accompagnée du texte de la disposition sur laquelle le refus s'appuie, le cas échéant, et d'un avis l'informant du recours en révision et indiquant notamment le délai dans lequel il peut être exercé;
- Veiller à ce que le renseignement faisant l'objet de la demande soit conservé le temps requis pour permettre au requérant d'épuiser les recours prévus à la loi.

- Supervise la tenue des registres énumérés de la présente Politique;
- Participe à l'évaluation du risque de Préjudice sérieux lié à un Incident de confidentialité, notamment eu égard à la sensibilité des renseignements visés, aux conséquences anticipées de leur utilisation et à la probabilité que ces renseignements soient utilisés à des fins malveillantes;
- Le cas échéant, effectue des vérifications des obligations de confidentialité en lien avec la communication de Renseignements personnels dans le cadre de mandats ou de contrats de service confiés à des tiers conformément à la présente Politique.

## 17.2 Le Comité

- Veille à la mise en place de mesures visant la sensibilisation et la formation des membres du personnel et des membres de la direction de la MRC sur les obligations et les pratiques en matière d'accès à l'information et de protection des Renseignements personnels;
- Élabore les principes de diffusion de l'information;
- Approuve la présente *Politique sur l'accès aux documents de la MRC et sur la protection des renseignements personnels, en lien avec la Loi modernisant des dispositions législatives en matière de protection de renseignements personnels (Loi 25)*;
- Émet des directives sur l'utilisation d'outils informatiques marketing impliquant la communication de données ou le Profilage;
- Identifie les principaux risques en matière de protection de Renseignements personnels et en avise la Direction générale de la MRC afin que des mesures correctives soient proposées;
- Approuve toute dérogation aux principes généraux de protection des Renseignements personnels qui auront été établis;
- Émet des directives pour la protection des Renseignements personnels, notamment pour la conservation de ceux-ci par des tiers et à l'extérieur du Québec;

- Est consulté, dès le début d'un projet et aux fins de l'ÉFVP, pour tous les projets d'acquisition, de développement et de refonte des systèmes d'information ou de prestation électronique de services impliquant des Renseignements personnels :
  - Veille à ce que la réalisation de l'ÉFVP soit proportionnée à la sensibilité des renseignements concernés, aux fins auxquelles ils sont utilisés, à la quantité et à la distribution des renseignements et au support sur lequel ils seront hébergés;
  - Le cas échéant, s'assure que le projet permet de communiquer à la Personne concernée les Renseignements personnels informatisés recueillis auprès d'elle dans un format technologique structuré et couramment utilisé;
- Escalade les recommandations qui ne sont pas suivies au RPRP;
- Doit être avisé de tout Incident de confidentialité impliquant les Renseignements personnels et conseiller la MRC quant aux suites à y donner;
- Revoit le *Formulaire de déclaration d'un Incident de confidentialité* dans l'éventualité d'un Incident de confidentialité;
- Revoit les règles pour la collecte et la conservation des Renseignements personnels provenant de sondages, y compris dans le cadre d'une politique de la MRC relative aux sondages;
- Revoit toute question d'intérêt touchant la protection des Renseignements personnels;
- Revoit les mesures relatives à la vidéosurveillance et s'assure du respect de la vie privée dans le cadre de son utilisation.

## 17.3 Traitement par les employés

Toute personne qui traite des Renseignements personnels que la MRC détient :

- Agit avec précaution et intègre les principes énoncés à la présente Politique à ses activités;
- N'accède qu'aux renseignements nécessaires à l'exercice de ses fonctions;
- N'intègre et ne conserve des renseignements que dans les dossiers destinés à l'accomplissement de ses fonctions;
- Conserve ces dossiers de manière à ce que seules les personnes autorisées y aient accès;
- Protège l'accès aux Renseignements personnels en sa possession ou auxquels elle a accès par un mot de passe;
- S'abstient de communiquer les Renseignements personnels dont elle prend connaissance dans l'exercice de ses fonctions, à moins d'être dûment autorisée à le faire;
- S'abstient de conserver, à la fin de son emploi ou de son contrat, les Renseignements personnels obtenus ou recueillis dans le cadre de ses fonctions et maintient ses obligations de confidentialité;
- Détruit tout Renseignement personnel conformément à la directive de destruction de la MRC;
- Participe aux activités de sensibilisation et de formation en matière de protection des Renseignements personnels qui lui sont destinées;

- Signale tout manquement, Incident de confidentialité ou tout autre situation ou irrégularité qui pourrait compromettre de quelque façon que ce soit la sécurité, l'intégrité ou la confidentialité de Renseignements personnels conformément à la procédure établie par la MRC.

# 18. DIRECTIVE ET FORMATION

## 18.1 Des employés

- Rapporter tout bris de confidentialité au RPRP afin qu'il produise l'avis de bris de confidentialité pour la CAI et qu'il contacte les Personnes concernées;
- Tout document papier contenant des Renseignements personnels devra être placé dans une salle ou un classeur fermé à clé;
- Le courrier ne doit être ouvert que par la personne à qui ce courrier est adressé;
- Les personnes responsables de la réception des informations dans le cadre d'embauche de personnel (concours) ne doivent partager ces informations papier et numérique qu'avec les membres du comité de sélection nommés par le directeur général de la MRC;
- L'employé qui imprime ou numérise un document contenant des Renseignements personnels confidentiels doit s'assurer de récupérer rapidement et de sécuriser le document original et sa copie papier et/ou numérique;
- Qu'elles soient émises par des journalistes, des spécialistes, des chercheurs ou des citoyens, les demandes d'accès à l'information verbale et/ou aux documents de la MRC doivent être analysées par le RAD avant d'être répondues. Il revient au RAD d'émettre une réponse écrite aux demandeurs, selon les délais prescrits par la Loi;
- Un document de référence concernant les Renseignements personnels confidentiels sera remis à chaque employé dès son entrée en poste, afin qu'il puisse évaluer par lui-même s'il peut communiquer ou non les informations demandées par un tiers. En cas de doute, il sera toujours possible de se référer au RPRP.

## 18.2 Utilisation des outils technologiques

- Le mot de passe du bureau informatique de l'employé doit être modifié tous les trois mois;
- Le mot de passe informatique ne doit pas être partagé entre les collègues. Si une situation demande un partage de mot de passe (p. ex. pour un soutien informatique, pour un soutien administratif), l'utilisateur doit changer dès que possible son mot de passe au retour à son poste;
- Lorsque l'utilisateur quitte son poste informatique, même pour une courte période, il doit verrouiller son écran, à l'aide des touches *Windows* + L. Une mise en veille est programmée lorsque le poste informatique n'est plus utilisé depuis cinq minutes;
- Lorsque l'employé est en télétravail, il doit s'assurer que les données verbales, manuscrites et informatiques ne sont pas accessibles à son entourage;
- Lorsque l'employé est en télétravail, en utilisant son poste informatique à distance, il doit s'assurer au préalable que tous ses écrans sont fermés à son poste informatique initial;

- Lorsque le cellulaire, qui n'est ni prêté ni payé par la MRC, est utilisé pour effectuer des appels aux collègues, aux municipalités, aux partenaires, il est préférable de désactiver la fonction d'affichage de numéro afin que soit affiché un appel privé et ainsi protéger le Renseignement personnel confidentiel de l'employé.
- En ce qui concerne la vie privée de l'employé utilisant les outils technologiques de la MRC, la *Politique régissant l'utilisation du système informatique de la MRC* est un document complémentaire à la présente Politique.

## 19. SANCTIONS

Toute personne qui enfreint la présente Politique est passible de sanctions selon le cadre normatif applicable.

## 20. MISE À JOUR

De manière à suivre l'évolution du cadre normatif applicable en matière de protection des Renseignements personnels et à améliorer le programme de protection des Renseignements personnels de la MRC, la présente Politique pourra être mise à jour au besoin. Veuillez-vous rendre à la version sur le site Web de la MRC pour consulter la version la plus récente.

## 21. ENTRÉE EN VIGUEUR

Cette *Politique sur l'accès aux documents de la MRC et sur la protection des renseignements personnels* s'applique à partir du moment où elle a été approuvée par résolution adoptée par le conseil de la MRC des Maskoutains et demeure en force tant qu'elle n'est pas modifiée par ce conseil.

Signé à Saint-Hyacinthe, le 12 octobre 2023.

Le directeur général,

André Charron, GMA

# Annexe A
# Modèle de registre des Incidents de confidentialité

Registre_incident_confidentialite_VF.pdf

Maskoutains

IMPRIMER

**FORMULAIRE DE DÉCLARATION**
**D'UN INCIDENT DE CONFIDENTIALITÉ**

RÉINITIALISER

Ce modèle de registre des incidents de confidentialité constitue un outil que la MRC des Maskoutains peut employer pour l'application de l'article 63.11 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de l'article 7 du Règlement sur les incidents de confidentialité.

Il doit également être possible d'y repérer facilement les incidents de confidentialité, notamment dans le cas où la Commission d'accès à l'information voudrait obtenir une copie du registre.

RAPPEL :

On entend par « incident de confidentialité » :

- l'accès non autorisé par la loi à un renseignement personnel;
- l'utilisation non autorisée par la loi d'un renseignement personnel;
- la communication non autorisée par la loi d'un renseignement personnel;
- la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Tous les incidents de confidentialité doivent être inscrits dans le registre des incidents de confidentialité, et cela, peu importe leur ampleur ou leur risque de préjudice. Si un incident présente un risque qu'un préjudice sérieux soit causé, l'organisme public doit, avec diligence, aviser la Commission d'accès à l'information. Il doit également viser toute personne dont un renseignement personnel est concerné par l'incident.

Maskoutains

**MODÈLE DE REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ**

| | | |
|---|---|---|
| Numéro de l'incident | | |
| Renseignements visés par l'incident | Décrire les renseignements personnels visés par l'incident ou en dresser une liste. Si cette information n'est pas connue, il faut le préciser et expliquer la raison qui justifie l'impossibilité de fournir une telle description. | |
| Circonstances de l'incident | Décrire brièvement les circonstances de l'incident. | |
| Date ou période de l'incident | Mentionner la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation : | |
| Date ou période de la prise de connaissance de l'incident | Mentionner la date ou la période au cours de laquelle la MRC des Maskoutains a pris connaissance de l'incident : | |
| Nombre de personnes concernées par l'incident | Mentionner le nombre de personnes concernées par l'incident ou, si ce dernier n'est pas connu, une approximation | |
| Risque qu'un préjudice sérieux soit causé | ◯ Oui ◯ Non<br>Décrire les éléments qui amènent la MRC des Maskoutains à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées. | |



Maskoutains

**MODÈLE DE REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ**

| | |
|---|---|
| Transmission des avis à la Commission d'accès à l'information et aux personnes concernées | Date(s) de l'avis à la Commission d'accès à l'information :<br>S'il y a un risque qu'un préjudice sérieux soit causé, inscrire la ou les dates. Sinon, inscrire « Sans objet ».<br>Date :<br>☐ Sans objet |
| | Date(s) de l'avis aux personnes concernées :<br>S'il y a un risque qu'un préjudice sérieux soit causé, inscrire la ou les dates. Sinon, inscrire « Sans objet ».<br>Date :<br>☐ Sans objet |
| | Avis public : ◯ Oui ◯ Non |
| | Si un avis public a été diffusé, en expliquer la raison. Dans le cas contraire, inscrire « Sans objet ».<br>Raison :<br>☐ Sans objet |
| Description des mesures prises par la MRC des Maskoutains | Décrire brièvement les mesures prises par la MRC des Maskoutains, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.<br>*Expliquez :* |

**Annexe B**

**Formulaire de déclaration d'un Incident de confidentialité**

Avis_incident_confidentialite_Formulaire_MRC_2023-08-07.pdf

Envoyer - Greffiere

MRC des Maskoutains
Un monde à votre mesure

**Section réservée à la MRC des Maskoutains**

Numéro de dossier : _____

Date de réception : _____

# FORMULAIRE DE DÉCLARATION D'UN INCIDENT DE CONFIDENTIALITÉ

Effacer formulaire

**Objet du présent formulaire**

Ce formulaire vise à permettre à la MRC des Maskoutains d'aviser la Commission d'accès à l'information de tout incident de confidentialité impliquant un renseignement personnel qu'elle détient et présentant un risque de préjudice sérieux.

On entend par « incident de confidentialité » :

- l'accès non autorisé par la loi à un renseignement personnel;
- l'utilisation non autorisée par la loi d'un renseignement personnel;
- la communication non autorisée par la loi d'un renseignement personnel;
- la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Soyez avisé(e) que les informations inscrites dans le présent formulaire sont soumises à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.* Ainsi, certains renseignements, dont le nom de la MRC et le fait qu'un incident l'impliquant est survenu, pourraient être communiqués publiquement.

Si vous manquez d'espace dans l'un des champs, joignez une annexe présentant l'ensemble de votre réponse lorsque vous transmettez le formulaire à la Commission et inscrivez « Voir annexe » dans le champ concerné.

## 1. Identification de l'organisation concernée par l'incident de confidentialité

| | |
|---|---|
| **A. Identification de l'organisme public** | |
| Nom : **MUNICIPALITÉ RÉGIONALE DE COMTÉ DES MASKOUTAINS** | |
| Adresse : 805, AVENUE DU PALAIS, SAINT-HYACINTHE, QUÉBEC, J2S 5C6 | |
| **Personne à contacter relativement à l'incident** | |
| Nom : MARIE-PIER HÉBERT | Fonction : GREFFIÈRE |
| Téléphone : 450 774-3141, poste 3116 | Courriel : greffier@mrcdesmaskoutains.ca |
| **Personne responsable de la protection des renseignements personnels** ☐ **Même que précédent** | |
| Nom : | Fonction : |
| Téléphone : | Courriel : |

## 2. Date et période de l'incident de confidentialité

| | |
|---|---|
| Date de l'incident : | Date de découverte de l'incident : |
| L'incident a eu lieu sur une période de : | |

## 3. Type d'incident de confidentialité

- ☐ Accès non autorisé par la loi à un renseignement personnel
- ☐ Utilisation non autorisée par la loi d'un renseignement personnel
- ☐ Communication non autorisée par la loi d'un renseignement personnel
- ☐ Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement

## 3.1 Causes et circonstances de l'incident de confidentialité

**Selon le type d'incident sélectionné ci-dessus, identifiez-la ou les cause(s) de celui-ci :**

| | | | |
|---|---|---|---|
| ☐ Altération délibérée | ☐ Communication accidentelle | ☐ Communication délibérée sans autorisation | ☐ Consultation non autorisée |
| ☐ Cyberattaque (virus, logiciel espion, etc.) | ☐ Défaillance technique | ☐ Destruction accidentelle | ☐ Destruction volontaire sans autorisation |
| ☐ Divulgation accidentelle | ☐ Divulgation délibérée sans autorisation | ☐ Erreur humaine | ☐ Hameçonnage (phishing) |
| ☐ Piratage (fraude) psychologique | ☐ Perte d'accès aux renseignements | ☐ Perte de renseignements | ☐ Rançongiciel |
| ☐ Utilisation incompatible | ☐ Vol de renseignements | ☐ Autre - *Précisez* : | |

**Selon le type d'incident sélectionné ci-dessus, décrivez les circonstances de celui-ci :**

MRC de Maskoutains

| Sur quel(s) support(s) les renseignements personnels étaient-ils conservés au moment de l'incident : | | |
|---|---|---|
| ☐ Ordinateur de bureau | ☐ Photo | ☐ Papier |
| ☐ Clé USB | ☐ Serveur | ☐ CD |
| ☐ Bande sonore | ☐ Téléphone portable | ☐ Infonuagique (cloud) |
| ☐ Tablette | ☐ Vidéosurveillance | ☐ Ordinateur portable |
| ☐ Dispositif amovible électronique | ☐ Autre - Précisez : | |

## 4. Description des renseignements personnels visés par l'incident de confidentialité

| | | |
|---|---|---|
| ☐ Nom<br>☐ Prénom | ☐ Adresse du domicile | ☐ Date de naissance ou<br>☐ Année ☐ Mois ☐ Jour ☐ Âge |
| ☐ Numéro de téléphone au domicile | ☐ Numéro du cellulaire | ☐ Adresse courriel personnelle |

| | |
|---|---|
| ☐ Numéro de permis de conduire | ☐ Numéro d'assurance sociale |
| ☐ Numéro d'assurance maladie | ☐ Numéro de passeport |
| ☐ Salaire | ☐ Fonction / occupation |

☐ Renseignements sur des employés, clients ou bénéficiaires - *Précisez :*

☐ Renseignements médicaux - *Précisez* :

☐ Renseignements génétiques - *Précisez* :

☐ Renseignements scolaires / académiques - *Précisez* :

☐ Renseignements bancaires / numéro de compte / institution / placements / hypothèque - *Précisez* :

| | | | |
|---|---|---|---|
| ☐ Numéro de carte de crédit | ☐ Numéro d'identification personnel (NIP) | ☐ Nom du détenteur | ☐ Code de sécurité à trois chiffres |
| ☐ Numéro de carte de débit | ☐ Numéro d'identification personnel (NIP) | ☐ Nom du détenteur | |

☐ Autres renseignements personnels - *Précisez* :

☐ Impossible de fournir une description des renseignements personnels visés - *Expliquez* :

## 5. Personnes concernées par l'incident de confidentialité

Nombre de personnes concernées par l'incident :

Nombre de personnes concernées par l'incident qui résident au Québec :

Si possible, ventilez le nombre de personnes concernées par l'incident selon leur lien avec la MRC des Maskoutains, qu'il s'agisse d'employés, de clients, d'étudiants, de patients, de membres, de bénévoles, de fournisseurs, etc., actuels ou anciens :

## 6. Évaluation du fait qu'un risque de préjudice sérieux puisse être causé aux personnes concernées par l'incident de confidentialité

Décrivez les éléments amenant la MRC à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées. Ce risque peut être attribuable au fait qu'il s'agisse de renseignements personnels sensibles ou à la possibilité que ces renseignements soient utilisés à des fins malveillantes ou préjudiciables. Dans ce cas, indiquez les conséquences appréhendées de leur utilisation sur les personnes concernées.

Décrivez les raisons qui supportent l'existence d'un risque de préjudice sérieux pour les personnes concernées par l'incident.

Le responsable de la protection des renseignements personnels de la MRC a-t-il été consulté pour procéder à l'évaluation du risque de préjudice?

☐ Oui ☐ Non

## 7. Avis aux personnes concernées

(Vous pouvez joindre une copie de l'avis transmis aux personnes concernées)

**La MRC a-t-elle avisé les personnes concernées par l'incident de confidentialité?**

☐ Non

☐ Oui. L'avis a été fait par :

| | | |
|---|---|---|
| ☐ Lettre transmise par courrier | ☐ Courriel | ☐ Message texte |
| ☐ Verbal (ex. par téléphone) | ☐ En personne | ☐ Autre - *Précisez* : |

Date de l'avis :

Si les personnes concernées n'ont pas encore été avisées, quelles mesures seront prises par la MRC afin de le faire?

| | | |
|---|---|---|
| ☐ Lettre transmise par courrier | ☐ Courriel | ☐ Message texte |
| ☐ Verbal (ex. par téléphone) | ☐ En personne | ☐ Autre - *Précisez* : |

Date de l'avis prévu :

☐ Aucune notification de l'incident aux personnes concernées n'est prévue. *Expliquez* :

## 7.1 Contenu de l'avis aux personnes concernées

**Sélectionnez les éléments contenus dans l'avis transmis aux personnes concernées par la MRC.**

- ☐ Une description des renseignements personnels visés par l'incident
- ☐ Une brève description des circonstances de l'incident
- ☐ La date ou la période où l'incident a eu lieu
- ☐ Une brève description des mesures que la MRC a prises ou entend prendre, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé
- ☐ Les mesures que la MRC suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice
- ☐ Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident

**Y a-t-il des personnes concernées par l'incident qui ne seront pas avisées par la MRC ?**

- ○ Non.
- ○ Oui. Combien :

*Expliquez* :

## 7.2 Avis public aux personne concernées

**L'avis aux personnes concernées a-t-il été fait, exceptionnellement, au moyen d'un avis public?**

- ○ Non
- ○ Oui. Sélectionnez la raison applicable :

☐ Le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée.

*Expliquez* :

☐ Le fait de transmettre l'avis est susceptible présenter une difficulté excessive pour la MRC.

*Expliquez* :

☐ La MRC n'a pas les coordonnées des personnes concernées.

*Expliquez* :

| Par quels moyens l'avis public a-t-il été fait? |
|---|
| ☐ Un avis dans les médias<br>Précisez lesquels :<br>Date de diffusion : |
| ☐ Un communiqué de presse<br>Date de diffusion : |
| ☐ Un avis sur le site Web de la MRC |
| ☐ Une conférence de presse<br>Lieu :<br>Date : |
| ☐ Une publication diffusée dans les médias sociaux - *Précisez lesquels* : |
| ☐ Autre - *Précisez* : |
| **Est-ce que la MRC a avisé d'autres autorités de protection des renseignements personnels à l'extérieur du Québec?** |
| ☐ Commissaire à la protection de la vie privée du Canada |
| ☐ Office of the information and privacy commissioner of Alberta |
| ☐ Office of the information and privacy commissioner of British Columbia |
| ☐ Commissaire à l'information et à la protection de la vie privée de l'Ontario |
| ☐ Autre - *Précisez* : |

## 8. Obligation de diminuer le risque de préjudice

| Quelles mesures ont été prise dès la découverte de l'incident, notamment afin de réduire les risques de préjudice aux personnes concernées? |
|---|
| |

| |
|---|
| Dans quel délai ces mesures ont-elles été prises? |
| |
| Est-ce que des mesures ont été prises après la découverte de l'incident afin d'éviter que de nouveaux incidents de même nature se reproduisent? |
| ◯ Non<br>◯ Oui. *Précisez* : |
| Y a-t-il des mesures prévues qui n'ont pas encore été prises? |
| ◯ Non<br>◯ Oui. Précisez : |
| Indiquez la date de mise en place des mesures prévues : |
| *La MRC des Maskoutains doit transmettre à la Commission tout renseignement relatif à l'incident de confidentialité dont elle prend connaissance après lui avoir transmis le présent avis. L'information complémentaire doit alors être transmise dans les meilleurs délais à compter de cette connaissance.* |
| Est-ce que des informations supplémentaires seront transmises à la Commission concernant l'incident rapporté? |
| ◯ Non<br>◯ Oui. *Précisez lesquelles et indiquez l'échéancier prévu* : |

| 9. Signature | |
|---|---|
| Prénom : | Nom : |
| Fonction : | Lieu : |
| Date de transmission du formulaire à la Commission : | |
| Pour le compte de la **Municipalité régionale de comté des Maskoutains** | |
| *Je déclare que les renseignements concernant l'incident de confidentialité fournis dans la présente déclaration sont complets et conformes aux faits.* | |
| Signature : | |

## BIBLIOGRAPHIE


ASSEMBLÉE NATIONALE DU QUÉBEC. *Projet de loi nº 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, sanctionné le 22 septembre 2021 [Fichier PDF], Éditeur officiel du Québec, 2021 [https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/Lois_et_reglements/LoisAnnuelles/fr/2021/2021C25F.PDF].

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *Aviser la Commission et les Personnes concernées* [en ligne], 2 mai 2023, [https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personnels/aviser-commission-et-personnes-concernees/].

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *Destruction et anonymisation,* [En ligne], 24 mai 2023, [https://www.cai.gouv.qc.ca/organismes/destruction-et-anonymisation/].

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *Espace évolutif – Modernisation des lois/La modernisation des Lois sur la protection des renseignements personnels au Québec,* [En ligne], 20 septembre 2022, [https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-Lois/].

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *Évaluer les risques,* [En ligne], 20 septembre 2022, [https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personnels/evaluer-risque/].

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *Prendre des mesures pour diminuer les risques*, [En ligne], 20 septembre 2022, [https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personnels/prendre-mesure-pour-diminuer-risques/].

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *Qu'est-ce qu'un renseignement personnel?*, [En ligne], 25 juillet 2023,[https://www.cai.gouv.qc.ca/quest-ce-un-renseignement-personnel/]

GOUVERNEMENT DU QUÉBEC. *Incident de confidentialité*, [En ligne], 23 février 2023, [https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/incident-de-confidentialite].

GOUVERNEMENT DU QUÉBEC. *Pratique recommandée en sécurité de l'information/Guide de catégorisation de l'information*, [Fichier PDF], Version 2.1, 2016, [https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/categorisation_information.pdf].

QUÉBEC. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels : RLRQ*, chapitre A-2.1, à jour au 1er avril 2023, [En ligne], Éditeur officiel du Québec, 2023, [https://www.legisquebec.gouv.qc.ca/fr/document/lc/A-2.1].

QUÉBEC. *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels : RLRQ*, chapitre A-2.1, r. 2, à jour au 1er juin 2023, [En ligne], Éditeur officiel du Québec, 2023, [https://www.legisquebec.gouv.qc.ca/fr/document/rc/A-2.1,%20r.%202%20/].